International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.2760

(05/2011)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS

Next Generation Networks – Security

Mobility security framework in NGN

Recommendation ITU-T Y.2760

International Telecommunication Union

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS

GLOBAL INFORMATION INFRASTRUCTURE	
General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899
INTERNET PROTOCOL ASPECTS	
General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899
IPTV over NGN	Y.1900–Y.1999
NEXT GENERATION NETWORKS	
Frameworks and functional architecture models	Y.2000–Y.2099
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Numbering, naming and addressing	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Network control architectures and protocols	Y.2500–Y.2599
Smart ubiquitous networks	Y.2600–Y.2699
Security	**Y.2700–Y.2799**
Generalized mobility	Y.2800–Y.2899
Carrier grade open environment	Y.2900–Y.2999
Future networks	Y.3000–Y.3099

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T Y.2760

Mobility security framework in NGN

Summary

Recommendation ITU-T Y.2760 specifies the mobility security framework in next generation network (NGN) transport stratum. It addresses the security requirements, security mechanisms and procedures for mobility management and control in NGN.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T Y.2760	2011-05-20	13

Keywords

Mobility security, NGN.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T Y.2760

Mobility security framework in NGN

1 Scope

This Recommendation describes the mobility security framework in next generation network (NGN) transport stratum. This Recommendation considers the security requirements in [ITU-T Y.2018]. This Recommendation includes authentication and key management, security context establishment, IP mobility security, and security of mobility management, control and transport in the transport stratum. This Recommendation addresses the scenarios including intra- and inter-technology mobility, intra- and inter-domain mobility.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T Q.1706] Recommendation ITU-T Q.1706/Y.2801 (2006), *Mobility management requirements for NGN*.

[ITU-T X.805] Recommendation ITU-T X.805 (2003), *Security architecture for systems providing end-to-end communications*.

[ITU-T Y.2011] Recommendation ITU-T Y.2011 (2004), *General principles and general reference model for Next Generation Networks*.

[ITU-T Y.2012] Recommendation ITU-T Y.2012 (2010), *Functional requirements and architecture of next generation networks*.

[ITU-T Y.2014] Recommendation ITU-T Y.2014 (2010), *Network attachment control functions in next generation networks*.

[ITU-T Y.2018] Recommendation ITU-T Y.2018 (2009), *Mobility management and control framework and architecture within the NGN transport stratum*.

[ITU-T Y.2701] Recommendation ITU-T Y.2701 (2007), *Security requirements for NGN release 1*.

[ITU-T Y.2704] Recommendation ITU-T Y.2704 (2010), *Security mechanisms and procedures for NGN*.

[ITU-T Y-Sup.7] ITU-T Y-series Recommendations – Supplement 7 (2008), *ITU-T Y.2000-series – Supplement on NGN release 2 scope*.

[ITU-R M.1645] Recommendation ITU-R M.1645 (2003), *Framework and overall objectives of the future development of IMT-2000 and systems beyond IMT-2000*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 handover (clause 6.2.2 of [ITU-T Q.1706]): The ability to provide services with some impact on their service level agreements to a moving object during and after movement.

3.1.2 horizontal mobility (clause 6.2.3 of [ITU-T Q.1706]): Mobility on the same layer as defined in [ITU-R M.1645]. Generally, it is referred to as the mobility within the same access technology.

3.1.3 mobility (clause 3.2 of [ITU-T Q.1706]): The ability for the user or other mobile entities to communicate and access services irrespective of changes of the location or technical environment.

3.1.4 NGN transport stratum (clause 3.10 of [ITU-T Y.2011]): That part of the NGN which provides the user functions that transfer data and the functions that control and manage transport resources to carry such data between terminating entities.

3.1.5 trust (clause 3.2.9 of [ITU-T Y.2701]): Entity X is said to trust entity Y for a set of activities if and only if entity X relies upon entity Y behaving in a particular way with respect to the activities.

3.1.6 vertical mobility (clause 6.2.3 of [ITU-T Q.1706]): Mobility between different layers as defined in [ITU-R M.1645]. Generally, it is referred to as the mobility between different access technologies.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 inter-technology mobility: See "Vertical mobility" in clause 3.1.

3.2.2 intra-technology mobility: See "Horizontal mobility" in clause 3.1.

3.2.3 security context: A set of security parameters including identifier, key material, key algorithm, etc.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

3G 3rd Generation

ABG-FE Access Border Gateway Functional Entity

AE Authentication Extension

AKA Authentication and Key Agreement

AM-FE Access Management Functional Entity

AN-FE Access Node Functional Entity

ANI Application to Network Interface

AR-FE Access Relay Functional Entity

DDoS Distributed Deny of Service

EAP Extensible Authentication Protocol

EN-FE Edge Node Functional Entity

FA Foreign Agent

HA	Home Agent
HDC-FE	Handover Decision Control Functional Entity
IP	Internet Protocol
L3HEF	Layer 3 Handover Execution Function
MIP	Mobile IP
MIPv4	Mobile IP for IP version 4. See [b-IETF RFC 3220]
MIPv6	Mobile IP for IP version 6. See [b-IETF RFC 3775]
MLM-FE	Mobile Location Management Functional Entity
MMCF	Mobility Management Control Functions
MN	Mobile Node
MOBIKE	IKEv2 Mobility and Multihoming Protocol. See [b-IETF RFC 4555]
NACF	Network Attachment Control Functions
NGN	Next Generation Network
NID-FE	Network Information Distribution Functional Entity
NNI	Network to Network Interface
PKI	Public Key Infrastructure
PMIPv6	Proxy Mobile IPv6. See [b-IETF RFC 5213]
RAN	Radio Access Network
RRP	Registration Reply
RRQ	Registration Request
TAA-FE	Transport Authentication and Authorization Functional Entity
TLM-FE	Transport Location Management Functional Entity
TLS	Transport Layer Security
TTLS	Tunnelled Transport Layer Security
TUP-FE	Transport User Profile Functional Entity
UE	User Equipment
UNI	User to Network Interface
WiMax	Worldwide Interoperability for Microwave Access
WLAN	Wireless LAN

5 Security requirements for mobility in NGN

NGN supports multiple access technologies, such as WLAN, WiMax, and 3G RAN, etc. [ITU-T Y.2012]. Mobility support is one of the features in NGN, which includes nomadicity and handover. In NGN release 2, handover covers inter-access networks and intra-access networks scenarios [ITU-T Y-Sup.7].

NGN supports the following features:

1) Trust model: NGN security trust model defines three security zones: trusted, trusted but vulnerable and un-trusted [ITU-T Y.2701]. It shows that access network has to go through the security gateway before accessing the core network.

2) NGN supports multiple access technologies.

3) NGN supports several mobility protocols, such as MIPv4, MIPv6, DSMIPv6, PMIPv6 and MOBIKE.

4) NGN supports multi-radio UE, such as WLAN, WiMax, 3G RAN, etc.

5) NGN supports service continuity when handover between heterogeneous access systems.

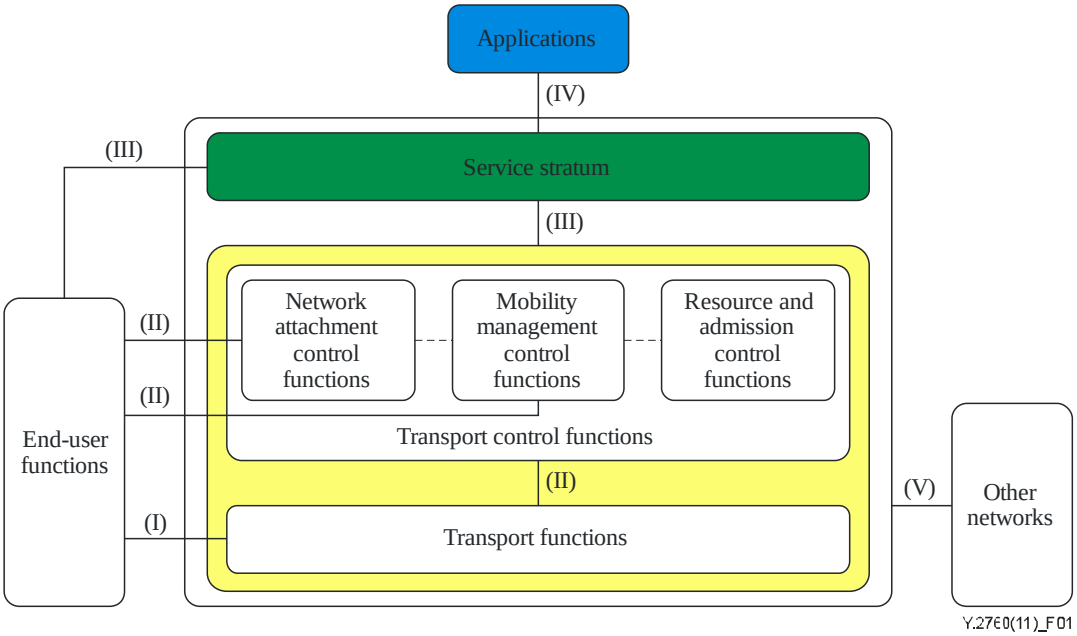

Figure 1 – Mobility security architecture in NGN

Five security feature groups are defined to:

(I) focus on security in transport layer between end-user functions and transport functions, such as access security which may be protected physically or logically between end-user functions and access network entity in transport functions. (I) also concerns the security of UNI between end-user functions and transport functions.

(II) focus on security in the control layer between end-user functions and the transport control function entity. (II) also focuses on security in the control message interface between transport functions entity and transport control function entity. (II) concerns the security of UNI between end-user functions and transport control functions.

(III) focus on security of interface between end-user functions and service stratum. (III) also focuses on security in control message interface between transport control functions entity and service stratum. (III) concerns the security of UNI between end-user functions and service stratum.

(IV) focus on security of interface between service stratum and application entity. (IV) concerns the security of ANI between end-user functions and transport functions.

(V) focus on security of interface between NGN and other networks which include both transport layer and control layer. (V) concerns the security of NNI between NGN network and other networks.

The principles of [ITU-T X.805] are applicable to the security threats and security requirements identified in this Recommendation.

5.1 Security threats

The following security threats are identified in [ITU-T Y.2018]:

T1 UE can be unauthorized to initiate the mobility signalling with MLM-FE.

T2 Mobility signalling can be tampered with by intruders.

T3 MLM-FE can be impersonated to provide false information to the UE.

T4 The UE location can be eavesdropped by intruders.

T5 Traffic redirection attack can happen.

T6 Attacker can insert itself on-path by man-in-the-middle attack.

T7 DDoS attack can consume a large quantity of network resources.

T8 UE can be unauthorized to get information from HDC-FE or NID-FE.

T9 HDC-FE or NID-FE can be impersonated to push false information to UE.

T10 The signalling between the UE and the HDC-FE or the NID-FE can be modified or eavesdropped.

T11 The user plane data can be eavesdropped or modified.

5.2 Security requirements

The following security requirements are identified in [ITU-T Y.2018]:

R1 The UE and NID-FE are required to be mutually authenticated.

R2 Signalling between the UE and the MLM-FE is required to be integrity- and confidentiality-protected.

R3 Signalling between the UE and the MLM-FE is required to be protected against replay attacks.

R4 The location privacy of the UE is required to be provided.

R5 The UE and HDC-FE are required to be mutually authenticated.

R6 Signalling between the UE and the HDC-FE is required to be integrity- and confidentiality-protected.

R7 Signalling between the UE and the HDC-FE is required to be protected against replay attacks.

R8 Low-latency authentication and signalling protection is required to be provided.

R9 Security context transfer is required to be optimized.

R10 The mobility security solution is required to be media independent.

R11 Mechanisms are required to be available to protect user plane traffic between the UE and the EN-FE when the user profile so indicates.

In addition to the security requirements identified in [ITU-T Y.2018], the following security requirement is also concerned:

R12 The security for multi-connection is required to be supported.

6 Security capabilities supported by relevant function entities

The functional entities related to mobility security in NGN are as follows:

- Transport user profile functional entity (TUP-FE)
- Transport authentication and authorization functional entity (TAA-FE)
- Mobile location management functional entity (MLM-FE)
- Handover decision control functional entity (HDC-FE)

- Network information distribution functional entity (NID-FE)
- Access management functional entity (AM-FE)
- Layer3 handover execute function (L3HEF)
- Access node functional entity (AN-FE)

6.1 Transport user profile functional entity (TUP-FE)

The TUP–FE stores subscription authentication data such as key material, authentication methods and the user transport profile. The detailed functional description of TUP-FE refers to [ITU-T Y.2014].

6.2 Transport authentication and authorization functional entity (TAA-FE)

The TAA-FE retrieves authentication data and accesses authorization information from TUP-FE. The TAA-FE can also act as a proxy.

The detailed functional description refers to [ITU-T Y.2014].

6.3 Mobile location management functional entity (MLM-FE)

MLM-FE obtains authentication, authorization and accounting information from NACF, performs mutual authentication with the UE, and creates security association between the UE and the MLM-FE. The detailed functional description refers to [ITU-T Y.2018].

6.4 Handover decision control functional entity (HDC-FE)

HDC-FE is required to establish security association with the UE, and obtains a security key used for security association from TAA-FE via TLM-FE. The detailed functional description refers to [ITU-T Y.2018].

6.5 Network information distribution functional entity (NID-FE)

NID-FE is required to establish security association with the UE to protect information such as network selection information. NID-FE can obtain security information from TAA-FE via TLM-FE. The detailed functional description refers to [ITU-T Y.2018].

6.6 Access management functional entity (AM-FE)

The AM-FE forwards network access requests to the TAA-FE to authenticate the user, authorize or deny the network access, and retrieve user-specific access configuration parameters. AM-FE can reuse the network registration/authentication data for fast recovery without performing the whole procedures of the registration/authentication/configuration repeatedly. The detailed functional description refers to [ITU-T Y.2014].

6.7 Layer3 handover execute function (L3HEF)

L3HEF is required to establish security association with the UE to protect traffic between them. The detailed functional description refers to [ITU-T Y.2018].

NOTE – The security of L3HEF addresses the security requirement of user plane traffic protection between the UE and EN-FE.

6.8 Access node functional entity (AN-FE)

AN-FE is required to establish security association with the UE, and it obtains key material from TAA-FE via AM-FE. The detailed functional description refers to [ITU-T Y.2018].

7 Key management and authentication

7.1 Key management framework

Hierarchical key derivation mechanism is used for mobility security in NGN. There are several kinds of key material in NGN, e.g., root key, session key, etc. The root key is one kind of long-term credential stored securely (e.g., shared secret key or password). The session key is one kind of short-term key material that is generated based on root key. Both the UE and authentication entity in NGN (e.g., TAA-FE/TUP-FE) store shared root key.

Usually, session key material is generated based on root key and other key generation parameters such as negotiation information during authentication procedure. Session key material is used to protect signalling traffic and user traffic. Session key can be derived further. The key derivation mechanism depends on the specific cryptographic algorithm or protocol.

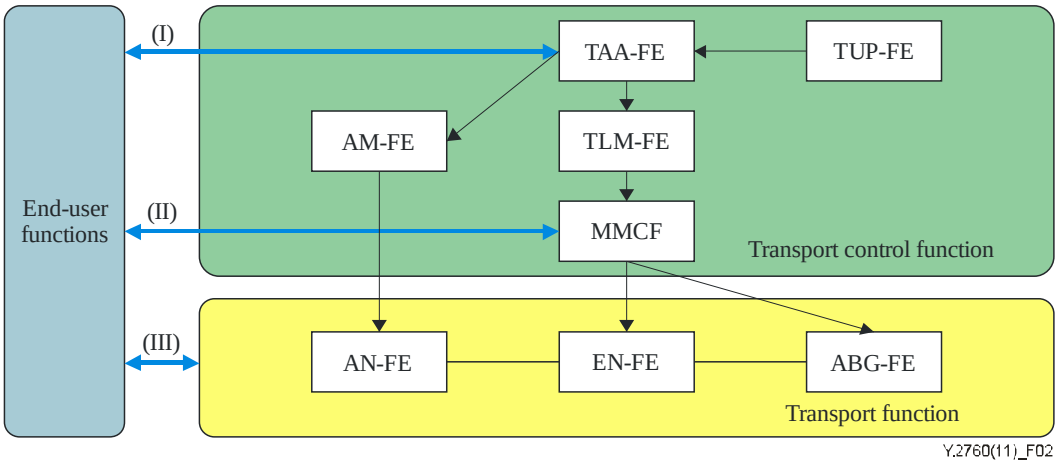

Figure 2 – Generic keying framework for mobility security in NGN

The generic keying framework for mobility security in NGN is described as follows:

(I) The UE performs mutual authentication procedure with function entities in NGN. In the authentication procedure, the TUP-FE generates authentication vectors based on root key material and sends these authentication vectors to TAA-FE. After the mutual authentication procedure has finished successfully, both the TAA-FE and the UE generate session key material. The session key material can be used to generate sub-session key material. The session key material is transferred to the function entities such as AM-FE, MMCF. Both AM-FE and MMCF can generate sub-session key materials based on the received session key material.

(II) The security associations for reference points between the UE and the MMCF are based on session key material from TAA-FE via TLM-FE. The session key material used in (II) is generated or derived according to session key material in TAA-FE.

(III) The security associations between the UE and the transport function layer in NGN are established based on shared key material which is generated from the previous session key material in TAA-FE, AM-FE or MMCF. AN-FE receives session key material from TAA-FE via AM-FE. If AM-FE has the capability of deriving session key material, AN-FE can get session key material from AM-FE directly. Both EN-FE and ABG-FE receive key material generated from TAA-FE via TLM-FE and MMCF. If MMCF has the capability of deriving session key material, both EN-FE and ABG-FE can get key material from MMCF.

The authentication procedure is based on challenge-response protocol, e.g., AKA [b-3GPP TS 33.102].

7.2 Authentication

7.2.1 Generic authentication procedure

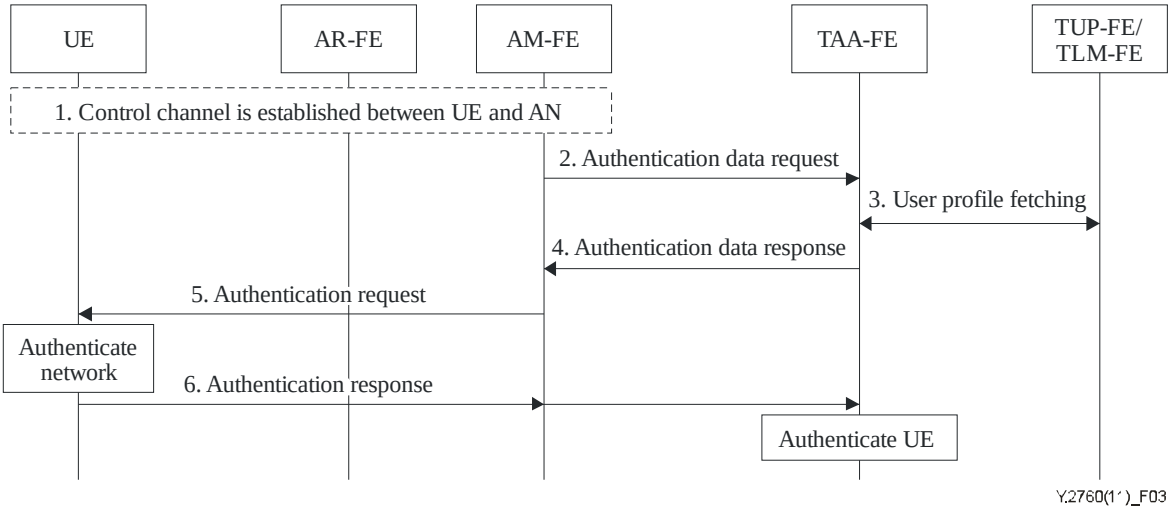

Figure 3 – Generic authentication procedure

1) The control channel between the UE and the access network functions is established (the procedure is out of the scope of this Recommendation).

2) The AM-FE sends the information of the UE to the TAA-FE to request authentication data.

3) The TAA-FE obtains the authentication information from the authentication request which includes user subscriber ID and access network information, interacts with the TUP-FE/TLM-FE to get user profile and authentication vectors including authentication token and session key material.

4) The TAA-FE sends the authentication data response including the authentication token to the AM-FE.

5) The AM-FE sends the authentication request to the UE. The UE fetches the authentication token from the authentication request, generates local authentication vectors including session key material based on authentication token and root key. The UE authenticates the network by validating the received authentication token.

6) The UE sends the authentication response to the AM-FE including the authentication token generated by the UE. The AM-FE forwards the information to the TAA-FE. The TAA-FE fetches the authentication token, checks the validation of the received authentication token to authenticate the UE.

7.2.2 Generic fast re-authentication procedure

Fast re-authentication is used to decrease handover latency. TUP-FE/TLM-FE is not involved in the fast re-authentication procedure, which makes the authentication procedure faster and reduces the load on the TUP-FE/TLM-FE. Both the UE and the authentication entities in NGN are recommended to support generic fast re-authentication.

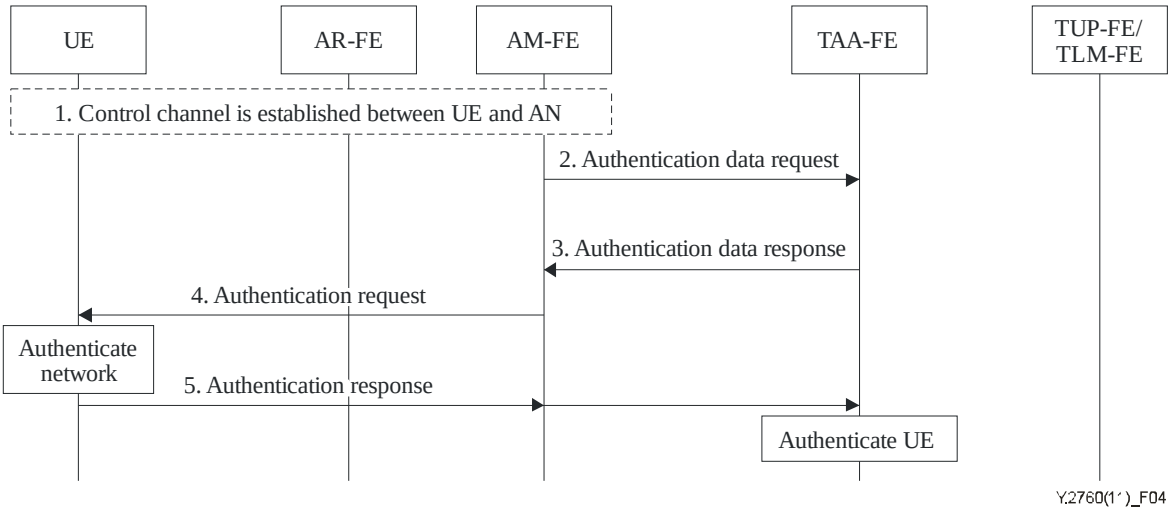

Figure 4 – Generic fast re-authentication procedure

The following steps are executed with the assumption that the UE and the TAA-FE have the capability of fast re-authentication.

1) The control channel between the UE and the access network functions is established (the procedure is out of the scope of this Recommendation).

2) The AM-FE sends the information of the UE to the TAA-FE to request authentication data.

3) The TAA-FE sends the authentication data response including the authentication token to the AM-FE.

4) The AM-FE sends the authentication request to the UE. The UE fetches the authentication token from the authentication request, generates local authentication vectors including session key material based on the authentication token and root key. The UE authenticates the network by validating the received authentication token.

5) The UE sends the authentication response to the AM-FE including the authentication token generated by the UE. The AM-FE forwards the information to the TAA-FE. The TAA-FE fetches the authentication token, checks the validation of the received authentication token to authenticate the UE.

When the UE reuses session key material, fast re-authentication information is only used for mutual authentication. When the UE does not reuse session key, both the UE and the authentication entity (e.g., TAA-FE/TUP-FE) generate a new session key based on session key material and fast re-authentication information.

7.2.2.1 Optimized fast re-authentication

For optimized fast re-authentication, a UE which has previously been authenticated by NGN generates authentication information. This procedure is different from generic re-authentication in that the UE first authenticates NGN and then NGN generates an authenticated token.

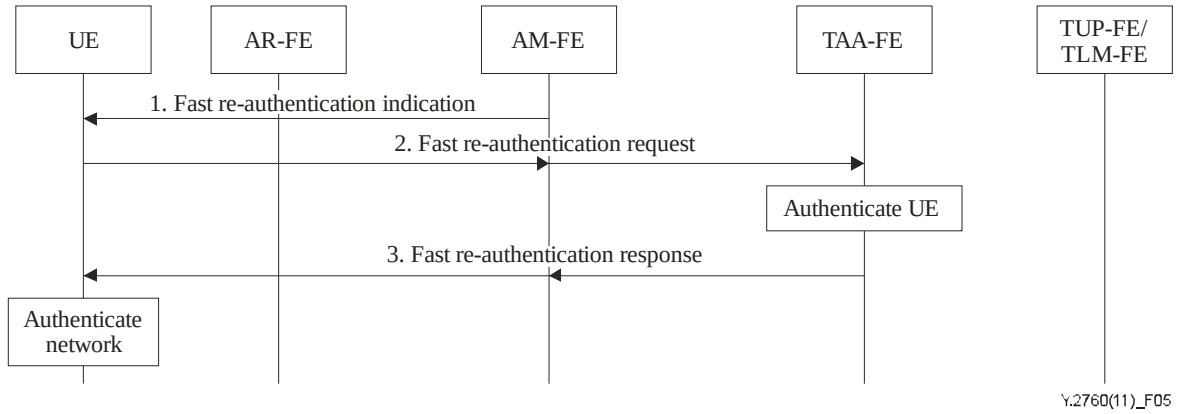

Figure 5 – Optimized fast re-authentication procedure

1) The control channel between the UE and the access network functions is established (the procedure is out of the scope of this Recommendation). The AM-FE sends optimized re-authentication indication to UE, which indicates that TAA-FE supports optimized fast re-authentication.

2) The UE generates the authentication vector and sends an optimized re-authentication request to the TAA-FE via the AM-FE. The optimized re-authentication request includes an authentication token and re-authentication information. The TAA-FE generates a local authentication vector and a new session key material based on the re-authentication information and session key material. The TAA-FE authenticates the UE by validating the received authentication token.

3) The TAA-FE sends the re-authentication response including the authentication token to the UE via the AM-FE. The UE authenticates the network by its own authentication vector. After authentication has finished successfully, the UE can generate a sub-session key material.

7.2.3 Intra-domain authentication

7.2.3.1 Authentication in single network connection

Single network connection means that the UE can detect a different network, but can access one network at a time. Pre-authentication means the UE mutually authenticates with a target network via the serving network before that UE makes a handover to the target network. When the UE is single network-connection based, the UE uses the pre-authentication to keep service continuity and lower latency. The pre-authentication procedure is similar to the generic authentication procedure. The serving AM-FE and the target AM-FE are involved in the pre-authentication procedure, if necessary.

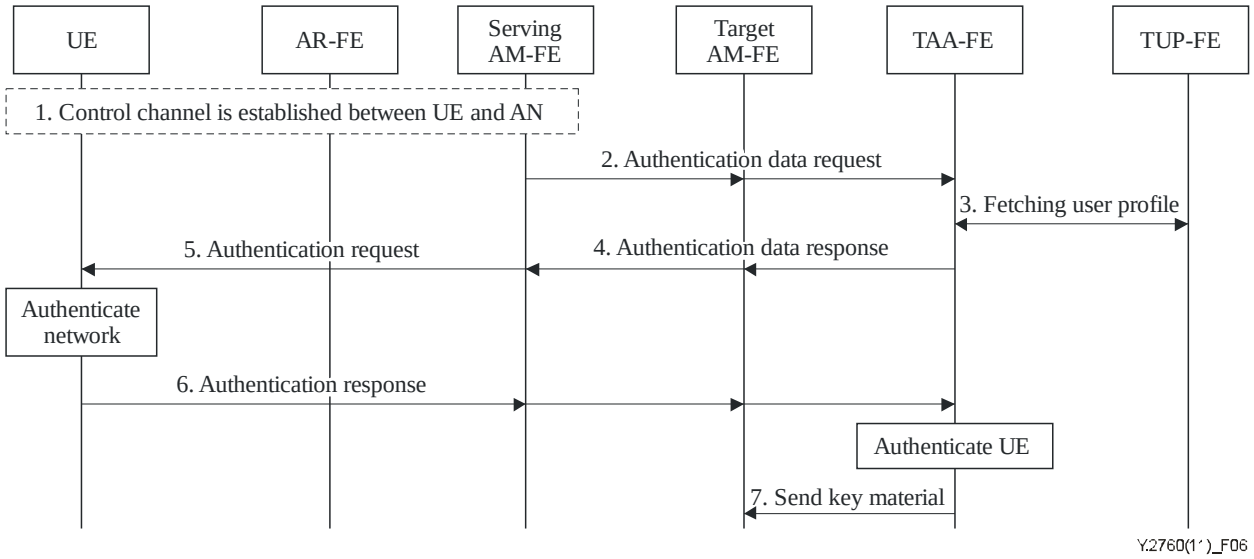

Figure 6 – Single network-connection based pre-authentication procedure

1) The control channel between the UE and access network functions is established (the procedure is out of the scope of this Recommendation).

2) AM-FE sends an authentication data request to the TAA-FE which includes subscriber information. The authentication data request is forwarded by the serving AM-FE and the target AM-FE.

3) The TAA-FE fetches the user profile by interacting with the TUP-FE.

4) The TAA-FE sends the authentication data response to the target AM-FE and the serving AM-FE including the authentication token.

5) The serving AM-FE sends the authentication request to the UE. The UE fetches the authentication token and authenticates the network by its own authentication information. After authentication has finished successfully, the UE generates a session key material.

6) The UE sends the authentication response to the serving AM-FE. The serving AM-FE forwards the information to the target AM-FE and TAA-FE including the authentication token. The TAA-FE retrieves the authentication token and authenticates the UE. After authentication has finished successfully, the TAA-FE generates a session key material which can derive a sub-session key material, if needed.

7) The TAA-FE sends the key material to the target AM-FE which will be used after the UE executes handover to the target network to protect communication between the UE and the target network.

7.2.4 Inter-domain authentication

A different administrative domain means a different NGN provider. An authentication procedure is described below for the UE handover between different administrative domains.

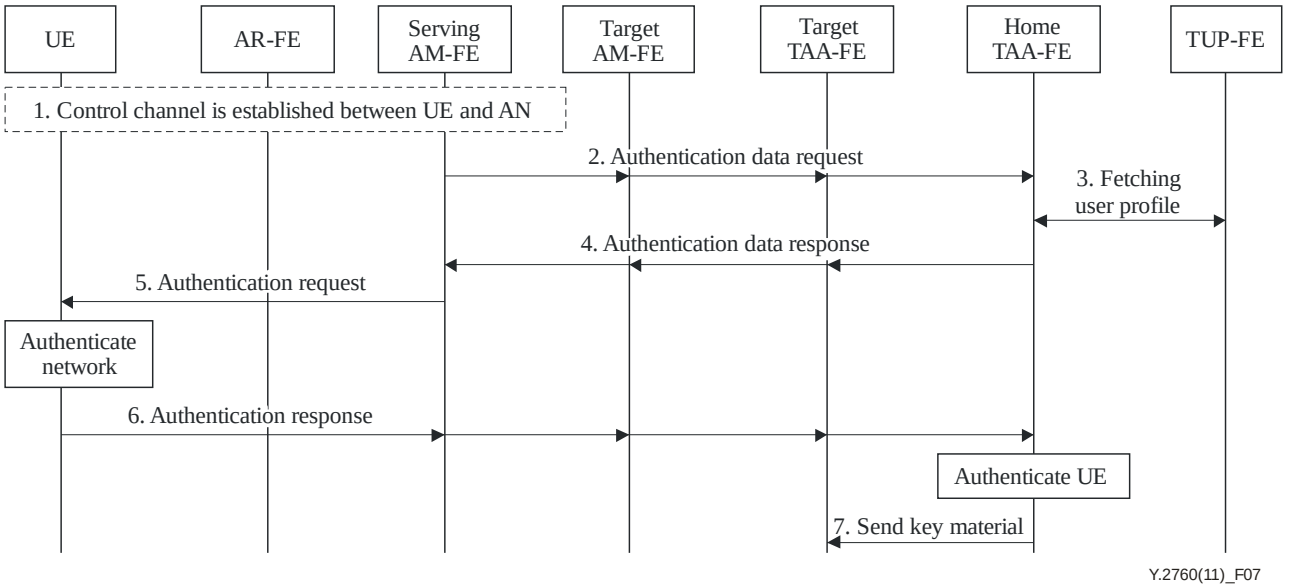

Figure 7 – Authentication procedure between different domains

1) The control channel between the UE and the access network functions is established (the procedure is out of the scope of this Recommendation).

2) The serving AM-FE sends the authentication data request to the home TAA-FE including subscriber information. The authentication data request is forwarded by the target AM-FE, and the target TAA-FE. The home TAA-FE fetches the user profile by interacting with the TUP-FE.

3) The TAA-FE fetches the user profile by interacting with the TUP-FE.

4) The home TAA-FE sends the authentication data response to the serving AM-FE including the authentication token. The authentication data response is forwarded by the target TAA-FE, and the target AM-FE.

5) The serving AM-FE sends the authentication request to the UE. The UE fetches the authentication token and authentication network by its own authentication information. After authentication has finished successfully, the UE generates a session key material.

6) The UE sends the authentication response to the home TAA-FE including the authentication token. The home TAA-FE retrieves the authentication token and authenticates the UE. After authentication has finished successfully, the home TAA-FE generates a session key material which can be used to derive a sub-session key material if needed.

7) After authentication has finished successfully, the home TAA-FE sends the key material to the target TAA-FE which is used after the UE executes the handover from the serving network to the target network to protect communication between the UE and the target network.

7.2.5 Key material mapping mechanism in authentication

When a UE moves from a serving network to a target network, mutual authentication is executed and session key material is generated. NGN supports different key derivation mechanisms and key material mapping is used to coordinate key material used for different key derivation mechanisms.

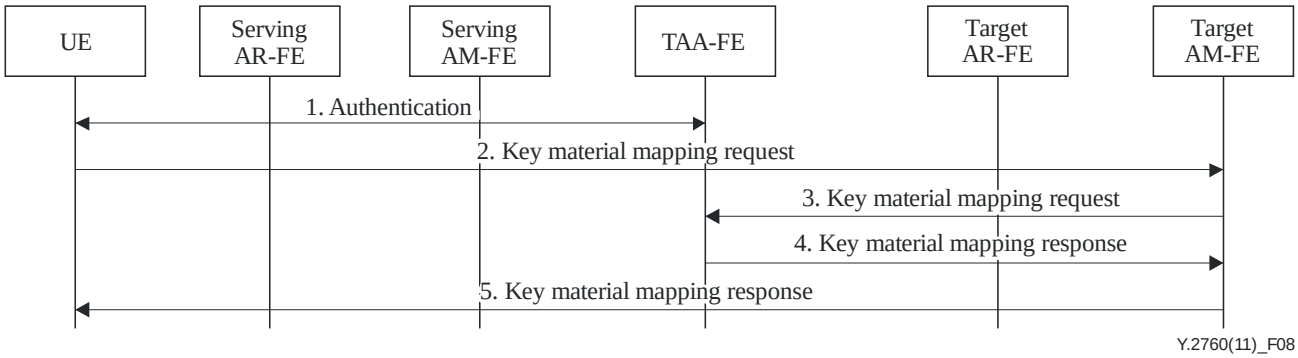

Figure 8 – Key material mapping procedure

1) Connection is established between the UE and the TAA-FE, the authentication procedure has finished and session key material is generated.

2) The UE detects a target network and prepares handover to the target network. The UE sends a key material mapping request to the target AM-FE. The key material mapping request includes mapping information such as current key derivation mechanism and supported key derivation mechanism.

3) The target AM-FE sends the key material mapping request to the TAA-FE.

4) The TAA-FE receives the key material mapping request and maps the key material in the serving network to key material in the target network, and sends the key material mapping response to the target AM-FE.

5) The target AM-FE sends the mapping response to the UE. The UE maps the key material in the serving network to the target key material in the target network. Both the UE and the TAA-FE have shared the target key material in the target network, which is used to protect traffic between the UE and the target network.

7.2.6 Multiple network access-based authentication

Multiple network access-based authentication means that the UE has the capability of communicating with multiple access networks simultaneously. When the UE has multiple network access capabilities, the UE connects to the target network and executes a mutual authentication procedure before disconnecting from the serving network. Mutual authentication is generic authentication, as depicted in Figure 3. After mutual authentication has finished successfully, both the UE and the TAA-FE generate a shared session key material, and the TAA-FE sends a session key material to the target AM-FE. When the UE moves to the target network, traffic between the UE and the target network is protected by the session key material or its sub-key material.

7.2.7 Multi-connection based authentication

Multi-connection means that the UE keeps more than one network connections simultaneously. Different types of network connections may provide users with different user experiences, such as broad bandwidth, low time delay, and high security. The case of multiple connections to different administrative domains is out of the scope of this Recommendation.

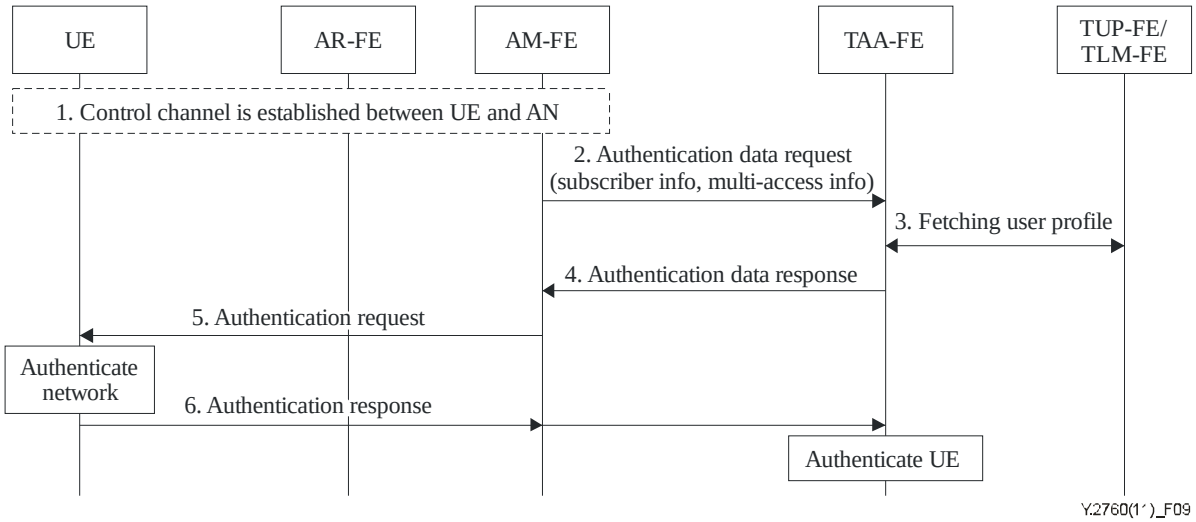

Figure 9 – Multi-connection based authentication

1) The control channel between the UE and the access network functions is established (the procedure is out of the scope of this Recommendation). The UE gets information from the access network and indication of supporting multi-access authentication.

2) The AM-FE sends an authentication data request to the TAA-FE. The authentication data request includes the UE information such as subscriber information (e.g., user subscriber ID); multi-access information (e.g., multi-access indication and multiple access interface ID).

3) The TAA-FE obtains the authentication information and interacts with the TUP-FE/TLM-FE to get user profile and authentication vector. An authentication vector is generated in the TUP-FE/TLM-FE. The authentication token is included in authentication vector.

4) TAA-FE sends the authentication data response, including the authentication token to the AM-FE.

5) The AM-FE sends the authentication request to the UE. The UE generates local authentication tokens based on the authentication information in the authentication request message. The UE authenticates the network by checking the validation of the received authentication token according to local authentication tokens. After authentication has finished successfully, the UE generates a session key material based on the authentication information. If multi-access indication is set, the UE generates multiple session key materials based on multi-access information.

6) The UE sends the authentication response message to the AM-FE. The AM-FE forwards the information to the TAA-FE including the authentication token generated by the UE. The TAA-FE fetches the authentication token in the authentication response message and authenticates the UE, based on the authentication vector in the TAA-FE. After authentication has finished successfully, the TAA-FE generates a session key material according to the authentication token. If multi-access indication is set, the TAA-FE generates multiple session key materials based on multi-access information.

8 Establishment of security context

8.1 Security context transfer between serving AM-FE and target AM-FE

The traffic of security context transfer between the serving AM-FE and the target AM-FE should be protected. The security between the serving AM-FE and the target AM-FE is achieved by establishing a security association. If the two AM-FEs are in the same zone, the security association

is not required. If the two AM-FEs are in a different zone, such as in different operator domains, the security association is created by the security mechanism and the operator's policy or agreement.

8.2 Security context transfer between serving AR-FE and target AR-FE

When the UE makes a handover between the serving AR-FE and the target AR-FE, the traffic of security context transfer between the target AR-FE and the serving AR-FE shall be protected. The security for security context transfer between the serving AR-FE and the target AR-FE is achieved by a establishing security association.

8.3 Security context transfer between UE and HDC-FE

8.3.1 Host-initiated security context transfer

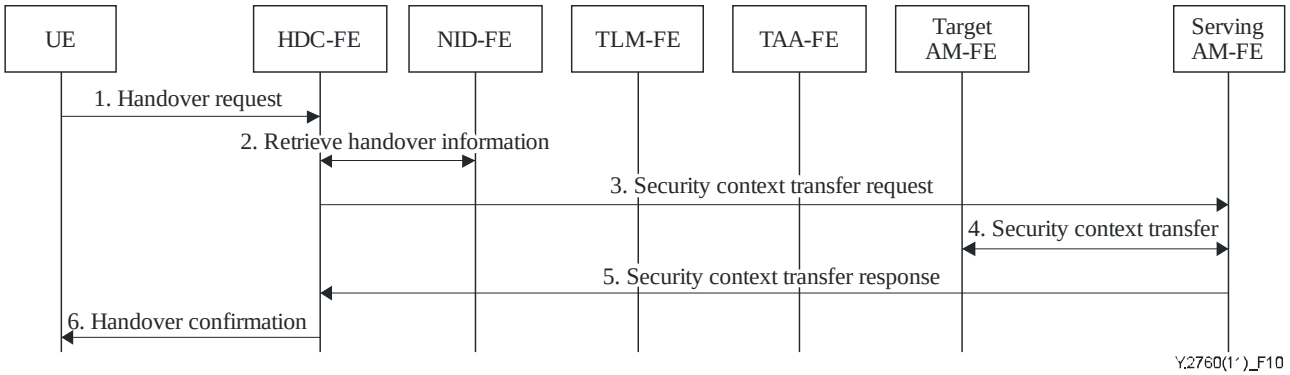

Figure 10 – Host-initiated security context transfer procedure

When the UE decides to achieve a handover from the serving network to the target network, the UE sends a handover request to the HDC-FE which triggers a security context transfer. After the security context transfer has finished, the target AM-FE uses the security context to protect the traffic between the UE and the target network. The steps are as follows:

1) The UE sends a handover request to the HDC-FE.

2) The HDC-FE receives the handover request, interacts with the NID-FE to get the handover-related information.

3) The HDC-FE forwards the handover request, including the handover-related information to the serving AM-FE.

4) The serving AM-FE interacts with the target AM-FE to transfer the security context.

5) When the security context transfer is finished, the serving AM-FE sends the security context transfer response to the HDC-FE.

6) The HDC-FE receives the security context transfer response. If the security context transfer has finished successfully, the HDC-FE sends the handover confirmation to the UE.

8.3.2 Network-initiated security context transfer

When the HDC-FE decides to trigger the UE to achieve a handover from the serving network to the target network, the HDC-FE sends a handover bootstrapping message to trigger security context transfer. After security context transfer has finished, the target AM-FE uses the security context to protect traffic between the UE and the target network.

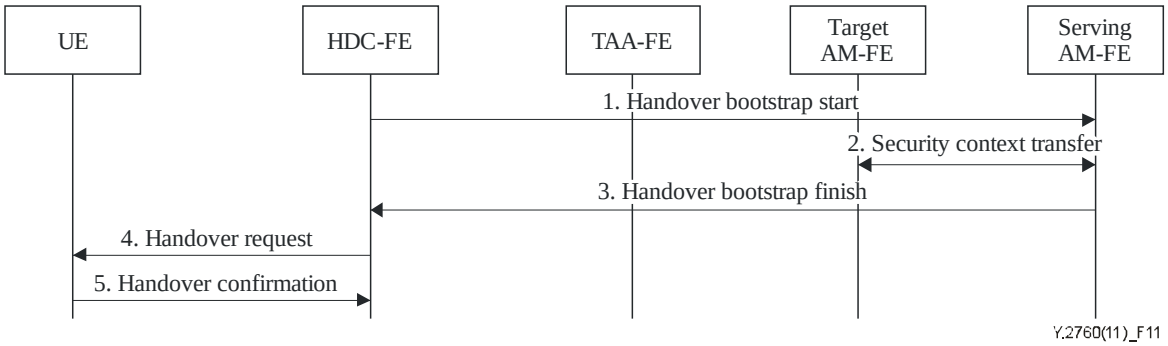

Figure 11 – Network-initiated security context transfer procedure

1) The HDC-FE prepares for handover procedure and sends a handover bootstrap start message to the serving AM-FE to trigger security context transfer.
2) The serving AM-FE interacts with the target AM-FE to transfer security context.
3) When security context transfer is finished, the serving AM-FE sends the handover bootstrap finish message to the HDC-FE.
4) When HDC-FE receives the handover bootstrap finish message, it begins the handover procedure by sending a handover request to the UE.
5) The UE sends the handover confirmation message when handover is finished.

9 IP mobility security

9.1 Host-based mobility security

Host-based mobility control traffic between the UE and MLM-FE (C) is required to be protected. The security association (SA) is required to be created between the UE and the MLM-FE(C). The SA between the UE and the MLM-FE (P) is optional.

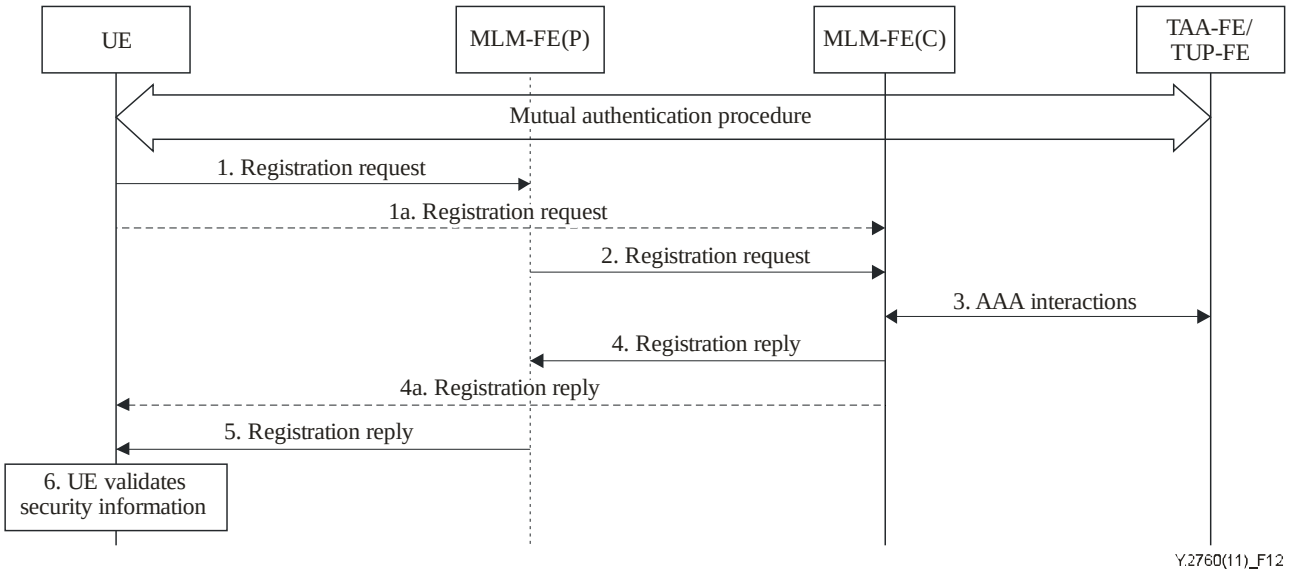

Figure 12 – Host-based mobility procedure

The following steps are executed with the assumption that the UE and the TAA-FE have finished the generic authentication procedure.

1) The UE sends a registration request to the MLM-FE(P). The registration request includes security information between the UE and the MLM-FE(C), and security information between the UE and MLM-FE(P).

   - 1a. If the MLM-FE(P) does not exist, the UE sends a registration request to the MLM-FE(C) directly.

2) The MLM-FE(P) validates the security information between the UE and the MLM-FE(P) and forwards the registration request to the MLM-FE(C). The MLM-FE(P) may add security information between the MLM-FE(P) and the MLM-FE(C) to the registration request message before forwarding it.

3) MLM-FE(C) interacts with TAA-FE/TUP-FE to get the authentication information and authorization information.

4) MLM-FE(C) validates the security information between the UE and the MLM-FE(C) in the registration request. The MLM-FE(C) sends the registration reply and security information to the MLM-FE(P). The registration reply may include security information between the UE and the MLM-FE(C), and security information between the MLM-FE(P) and the MLM-FE(C).

   - 4a. If MLM-FE (P) does not exist, MLM-FE(C) sends the registration reply to the UE directly. The registration reply may include security information between the UE and the MLM-FE(C).

5) MLM-FE(P) validates the security information between the MLM-FE(P) and the MLM-FE(C) and sends the registration reply to the UE. MLM-FE(P) may add security information between the UE and MLM-FE(P) to the registration reply message before forwarding it.

6) MLM-FE(C) validates the security information between the UE and the MLM-FE(C), and creates the SA between the UE and the MLM-FE(C). If the MLM-FE(P) exists, the UE validates the security information between the UE and the MLM-FE(P) and creates the SA between the UE and the MLM-FE(P).

9.2 Network-based mobility security

The protection for network-based mobility control traffic between two network entities in trust zone, or trust but vulnerable zone, is optional and based on the operator's policy. The security mechanisms for network-based mobility control traffic are based on security mechanisms in [ITU-T Y.2704].

10 Security between UE and HDC-FE

The information flow between the UE and the HDC-FE is used to carry information to make the handover decision. The UE and the HDC-FE should establish a security association to protect the information flow between the UE and the HDC-FE.

10.1 Host-initiated security association establishment between UE and HDC-FE

The host-initiated security association establishment procedure means that the UE triggers the procedure to create security association between the UE and the HDC-FE, which is depicted in Figure 13. There are two pre-conditions for host-initiated security association establishment between the UE and the HDC-FE. First, the UE and the TAA-FE have a pre-shared key material. The pre-shared key material can be achieved after mutual authentication procedure. Second, the UE knows the HDC-FE information, such as address, by which the UE sends a security association request to the HDC-FE. The way in which the UE obtains the HDC-FE information is out of the scope of this Recommendation. The TLM-FE is used to relay the key material information to/from the TAA-FE; this is omitted in the following figure.

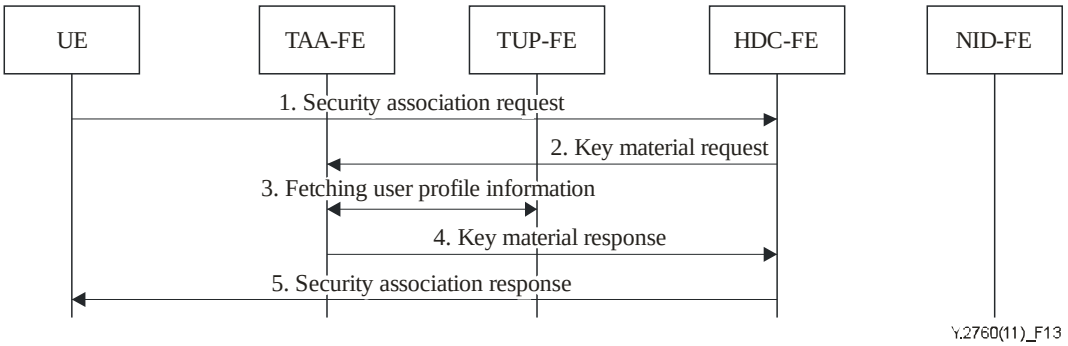

Figure 13 – Host-initiated security association establishment procedure

1) The UE generates a shared key material for creating an association with the HDC-FE, according to the authentication information. The UE sends the security association request to the HDC-FE, including authentication information and UE information.

2) The HDC-FE sends the key material request to the TAA-FE, including HDC-FE information, authentication information and UE information.

3) The TAA-FE fetches user profiles information by interacting with the TUP-FE and checks that HDC-FE is authorized to create a security association with the UE.

4) The TAA-FE generates key material for HDC-FE, according to authentication information, HDC-FE information, and UE information when the HDC-FE has authorization to create a security association with the UE. The TAA-FE sends a key material response to the HDC-FE, including such information as key material for HDC-FE, key lifetime.

5) The HDC-FE sends the security association response to inform that security association between UE and HDC-FE is established.

10.2 Network-initiated security association establishment between UE and HDC-FE

The network-initiated security association establishment procedure means that the network side triggers the procedure to create a security association between the UE and the HDC-FE, which is depicted in Figure 14. There are two pre-conditions for network-initiated security association establishment between the UE and the HDC-FE. First, the UE and the TAA-FE have a shared key material. The shared session key material can be generated after mutual authentication procedure. Second, the HDC-FE knows the UE information such as subscriber information or location information by which the HDC-FE sends the security association information to the UE. The way in which to get the UE information for HDC-FE is out of the scope of this Recommendation.

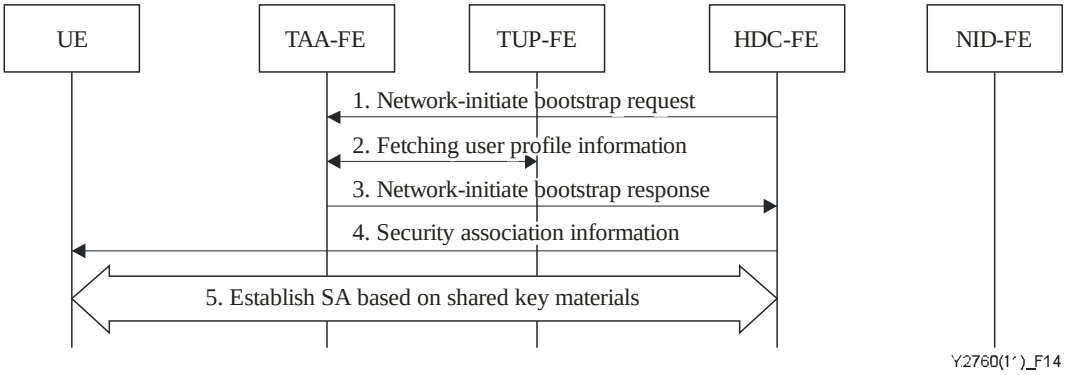

Figure 14 – Network-initiated security association establishment procedure

1) The HDC-FE sends a network-initiate bootstrap request to the TAA-FE, including HDC-FE information and UE information.

2) The TAA-FE fetches the user-profile information by interacting with the TUP-FE and checks that HDC-FE is authorized to initiate creating a security association with the UE.

3) The TAA-FE generates a key material for HDC-FE, according to HDC-FE information and UE information when HDC-FE has authorization to initiate creating a security association with the UE. TAA-FE sends the network-initiate bootstrap response to the HDC-FE, including the authentication information such as key material for HDC-FE and its lifetime.

4) HDC-FE sends the security association information, including authentication information to the UE to create a security association.

5) The UE generates key material for HDC-FE, according to the authentication information in security association information and validates the security association information. Security association is created between the HDC-FE and the UE.

10.3 Security association pre-establishment between UE and HDC-FE based on PKI

Security association establishment procedure between UE and HDC-FE based on PKI is depicted in Figure 15. The pre-condition for security association establishment procedure between UE and HDC-FE is that UE knows HDC-FE information, such as address by which UE sends security association request to HDC-FE. The way in which UE gets HDC-FE information is out of the scope of this Recommendation.

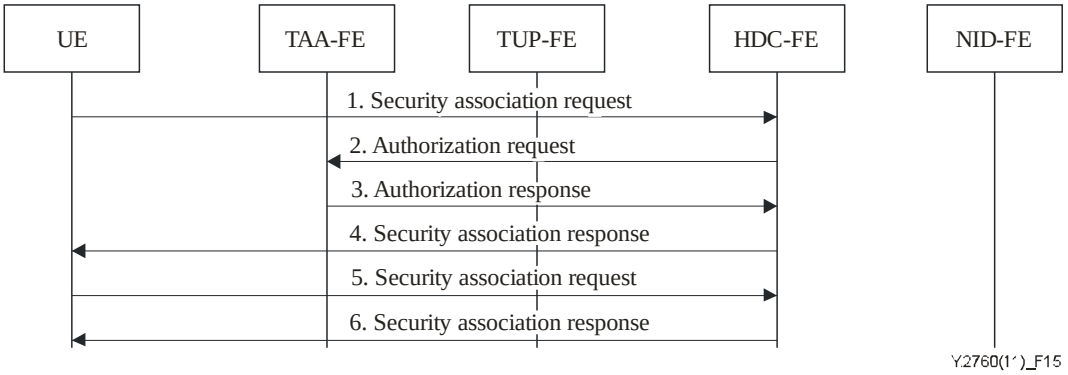

Figure 15 – Security association establishment procedure based on PKI

1) The UE sends a security association request to the HDC-FE, including UE certificate and UE information.

2) The HDC-FE validates the UE certificate and sends an authorization request, including UE information and HDC-FE information to the TAA-FE.

3) The TAA-FE checks the authorization based on UE information and HDC-FE information. If the UE is authorized to use HDC-FE, the TAA-FE sends an authorization response to the HDC-FE, including authorization information and server certificate.

4) The HDC-FE receives the authorization information and sends a security association response to the UE, including server certificate.

5) If a shared key material is needed between the UE and the TAA-FE, the TAA-FE sends key generation information to the UE in step 4. The UE generates a shared key material based on the received key generation information and local key generation information. The UE sends local key generation information to the HDC-FE.

6) The HDC-FE generates key material based on the received key generation information and local key generated information. The HDC-FE sends the security association response to the UE. Security association between the UE and the HDC-FE is established.

11 Security between UE and NID-FE

11.1 Host-initiated security association establishment between UE and NID-FE

Host-initiated security association establishment procedure between the UE and the NID-FE is depicted in Figure 16. The pre-conditions for security association establishment procedure between the UE and the NID-FE are as follows: 1) the UE and the TAA-FE have a shared key material. The shared session key material can be generated after mutual authentication procedure. 2) The UE knows NID-FE information, such as address by which the UE sends a security association request to the NID-FE. The way in which UE obtains NID-FE information is out of the scope of this Recommendation.

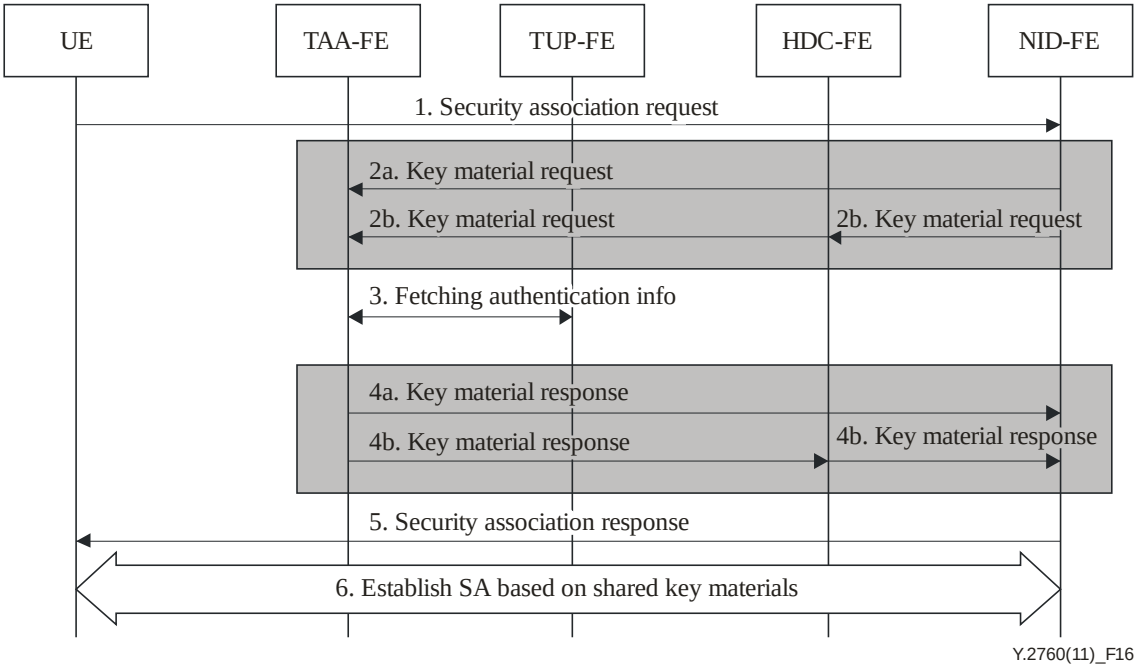

Figure 16 – Host-initiated security association establishment

1) The UE sends a security association request to the NID-FE.
2) The NID-FE sends a key material request to the TAA-FE, including NID-FE information and UE information. When the NID-FE does not support sending an authentication request to the TAA-FE directly, the NID-FE sends an authentication request to the TAA-FE via HDC-FE.
3) The TAA-FE interacts with the TUP-FE and generates key material for NID-FE.
4) The TAA-FE sends the key material response to the HDC-FE, including authentication information. Authentication information includes shared key material and its lifetime. When the TAA-FE does not support sending an authentication request to the NID-FE directly, the TAA-FE sends authentication request to the NID-FE via the HDC-FE.
5) The NID-FE sends the security association response, including authentication information to the UE protected by the shared key material.
6) The UE generates the shared key material and validates the security association response. Security association is created by the NID-FE and the UE based on the shared key material.

11.2 Network-initiated security association establishment between UE and NID-FE

Network-initiated security association establishment procedure between the UE and the NID-FE is depicted in Figure 17. The pre-conditions for security association establishment procedure between the UE and the NID-FE are as follows: 1) the UE and TAA-FE have a shared key material. The shared session key material can be generated after mutual authentication procedure. 2) The UE knows the NID-FE information such as address by which the UE sends the security association request to the NID-FE. The way in which the UE obtains the NID-FE information is out of the scope of this Recommendation.

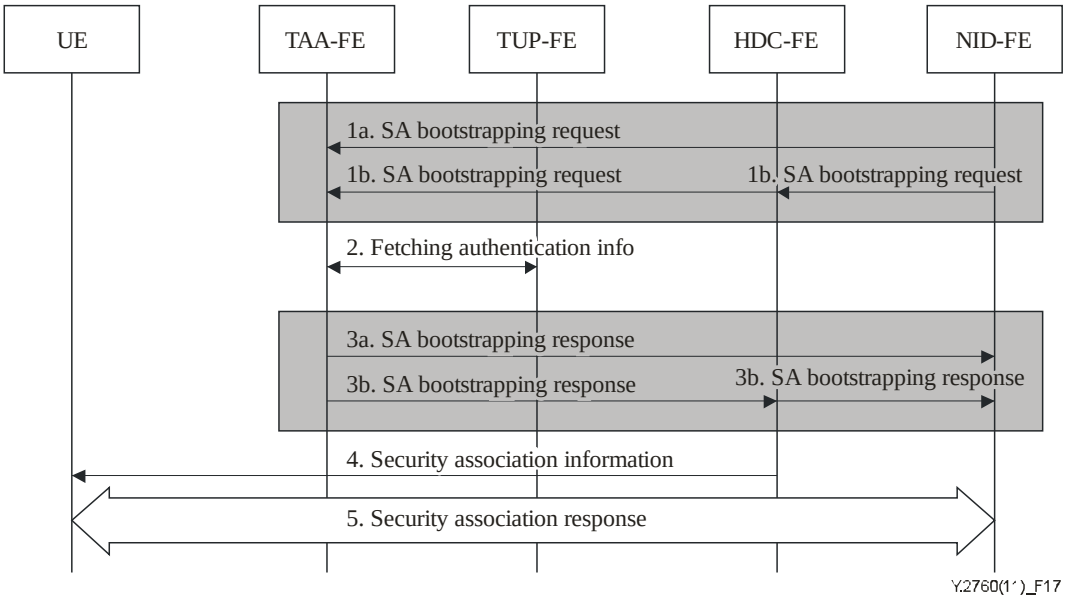

Figure 17 – Network-initiated security association establishment

1) The NID-FE sends a SA bootstrapping request to the TAA-FE, including NID-FE information. When the NID-FE does not support sending a SA bootstrapping request to the TAA-FE directly, the NID-FE sends a SA bootstrapping request to the TAA-FE via the HDC-FE.

2) The TAA-FE interacts with the TUP-FE and generates a key material for the NID-FE.

3) The TAA-FE sends a SA bootstrapping response to the NID-FE, including authentication information. The authentication information includes key material and its lifetime. When the TAA-FE does not support sending a SA bootstrapping response to the NID-FE directly, the TAA-FE sends a SA bootstrapping response to the NID-FE via the HDC-FE.

4) The NID-FE sends the security association information, including authentication information to the UE protected by the shared key material.

5) The UE generates the shared key material and validates the security association information. The security association is created by the NID-FE and the UE based on the shared key material.

11.3 Security association establishment between UE and NID-FE based on PKI

The security association establishment procedure between the UE and the NID-FE based on the PKI is depicted in Figure 18. The pre-condition for the security association establishment procedure between the UE and the NID-FE is that the UE knows NID-FE information, such as address by which the UE sends the security association request to the NID-FE. The way in which the UE obtains the NID-FE information is out of the scope of this Recommendation.

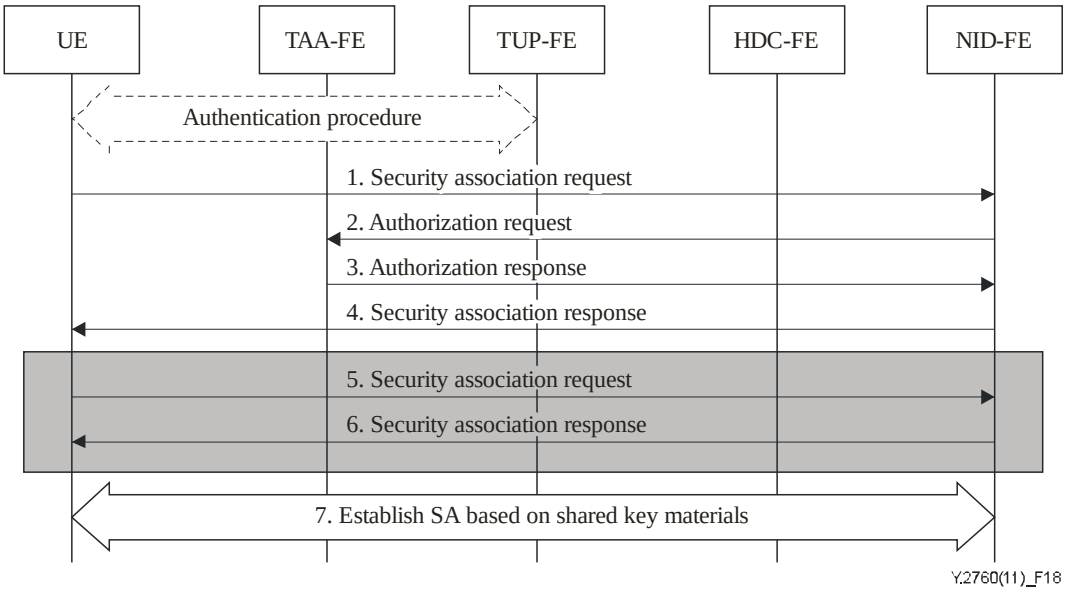

Figure 18 – Security association establishment procedure based on PKI

After the authentication procedure between the TUP-FE and the TAA-FE is completed, the following steps are performed:

1) The UE sends a security association request to the NID-FE, including the UE certificate and UE information.

2) The NID-FE validates the UE certificate and sends an authorization request, including UE information and NID-FE information, to the TAA-FE.

3) The TAA-FE checks the authorization based on the UE information and the NID-FE information. If the UE is authorized to use the NID-FE, the TAA-FE sends an authorization response to NID-FE, including authorization information and server certificate.

4) The NID-FE receives the authorization information and sends a security association response to the UE, including server certificate.

5) If a shared key material is needed between the UE and the TAA-FE, the TAA-FE sends the key generation information to the UE in step 4. The UE generates shared key material based on the received key generation information and the local key generation information. The UE sends the local key generation information to the NID-FE as part of a security association request.

6) The NID-FE generates the key material based on the received key generation information and the local key generated information. The NID-FE sends the security association response to the UE.

7) The security association between the UE and the NID-FE is established.

12 Security for transport functions

12.1 Security between UE and access node function entity

The traffic between the UE and the AN-FE should be protected. The security association between the UE and the AN-FE is based on the shared key material. When the authentication procedure between the UE and the TAA-FE has finished successfully, both the UE and the TAA-FE generate a key material such as session key for protecting traffic between the UE and the AN-FE. The TAA-FE sends the key material to the AN-FE via the AM-FE, and AR-FE.

12.2 Security between UE and L3HEF (Layer3 Handover Execute Function)

The traffic between the UE and the L3HEF should be protected. The security association between the UE and the L3HEF is based on the pre-shared key material. When mutual authentication is finished successfully, both the UE and the TAA-FE generate the key material such as session key for protecting traffic between the UE and L3HEF. L3HEF obtains the key material from TAA-FE directly. L3HEF also obtains the key material from the TAA-FE via the AM-FE or the HDC-FE.

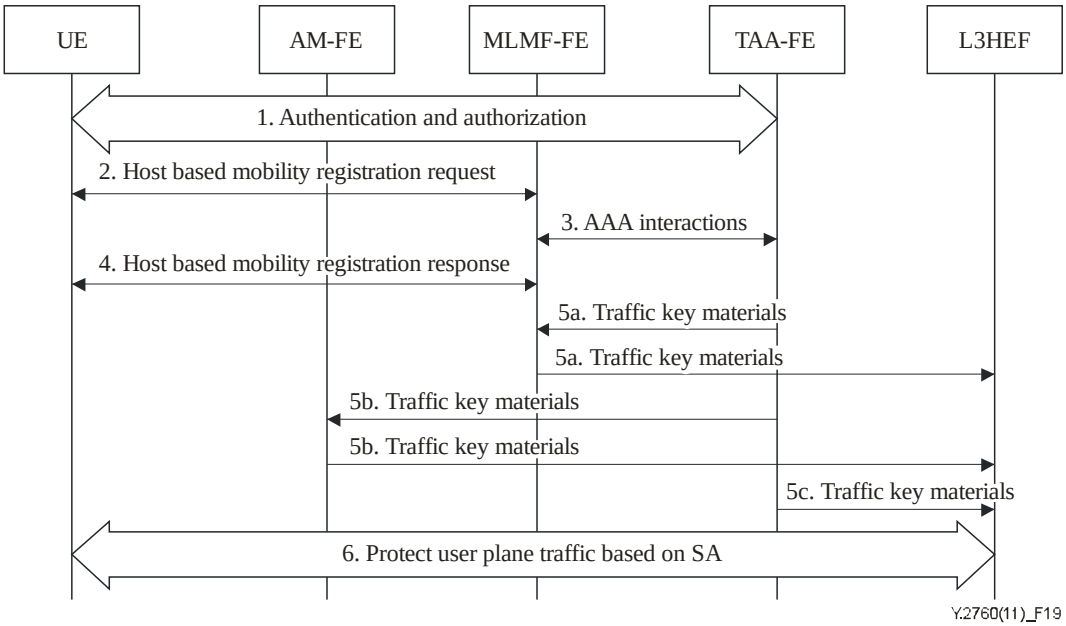

Figure 19 – User plane traffic security between UE and L3HEF procedure

1) Connection is established between the UE and the TAA-FE. After the mutual authentication is finished, the both UE and the TAA-FE have a shared key material such as transient key material and session key material.

2) The UE sends a host-based mobility registration request to the MLM-FE to create a host-based mobility security association.

3) The MLM-FE obtains the key material by interacting with the TAA-FE. The MLM-FE authenticates the UE based on the key material. After authentication has finished successfully, the MLM-FE creates a security association with the UE based on the key material.

4) The MLM-FE sends a host-based mobility registration response to the UE. The UE validates the host-based mobility registration response message and creates a security association with the MLM-FE.

5) After the security associations between the UE and the MLM-FE are created, three situations will have occurred:

   5a. The TAA-FE generates the traffic key material, and sends the traffic key material to the L3HEF via the MLM-FE.

   5b. The TAA-FE generates the traffic key material and sends the traffic key material to the L3HEF via the MLM-FE and the AM-FE.

   5c. The TAA-FE sends the traffic key material to the L3HEF directly.

6) The L3HEF uses the traffic key material to protect user plane traffic between the UE and the L3HEF.

Appendix I

(This appendix forms an integral part of this Recommendation.)

I.1 Example of full authentication procedure

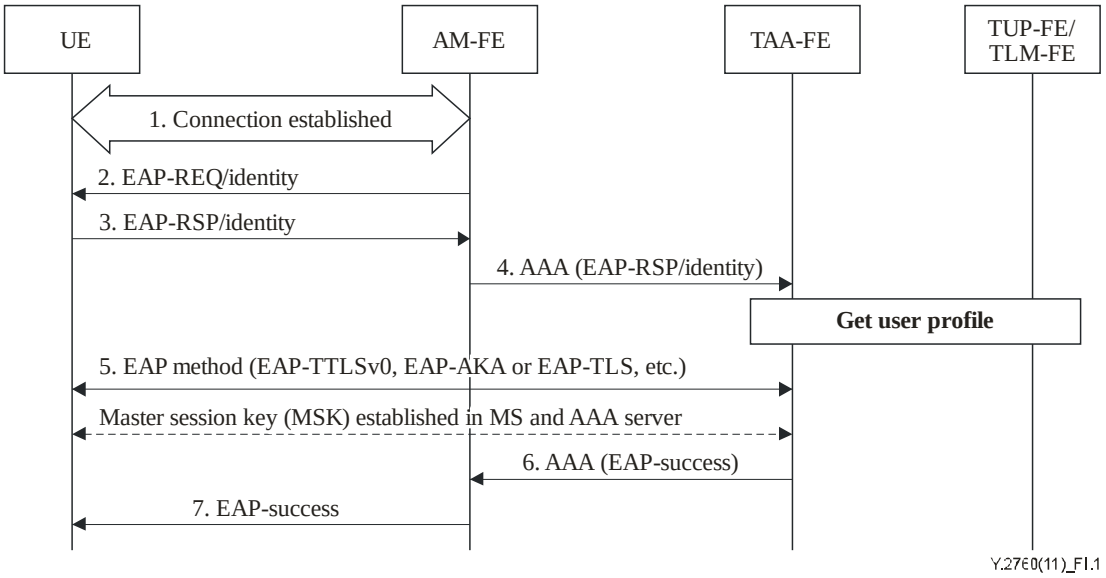

Figure I.1 – Full authentication procedure

NOTE – The identity in step 2-4 refers to UE Identity.

The bootstrapping for authentication is depicted in Figure I.1:

1) Connection is established between the UE and the AM-FE.
2) The AM-FE sends an EAP Request (EAP-REQ)/Identity to the UE [b-IETF RFC 3748].
3) The UE sends an EAP Response (EAP-RSP)/Identity message.
4) The AM-FE forwards the EAP-RSP/Identity towards the TAA-FE; afterwards, the TAA-FE exchanges information with TUP-FE/TLM-FE, and TUP-FE/TLM-FE sends user information, including the profile, to the TAA-FE.
5) The key derivation and distribution process are executed in the TAA-FE and the UE. Several methods can be considered, such as EAP-TTLS, EAP-AKA, EAP-TLS, etc.
6) The TAA-FE sends the EAP Success message to the AM-FE.
7) The AM-FE informs the UE of the successful authentication with the EAP Success message. Now the key exchange process, based on the EAP, has been successfully completed, and the UE and AM-FE share the keying material derived during that exchange.

I.2 Example of fast re-authentication procedure

When handover occurs, fast re-authentication can keep the continuity of service in low latency. Fast re-authentication needs to use a fast re-authentication id, and it does not need to exchange authentication information between the TAA-FE and the TUP-FE/TLM-FE.

The general procedure of fast re-authentication is shown as follows.

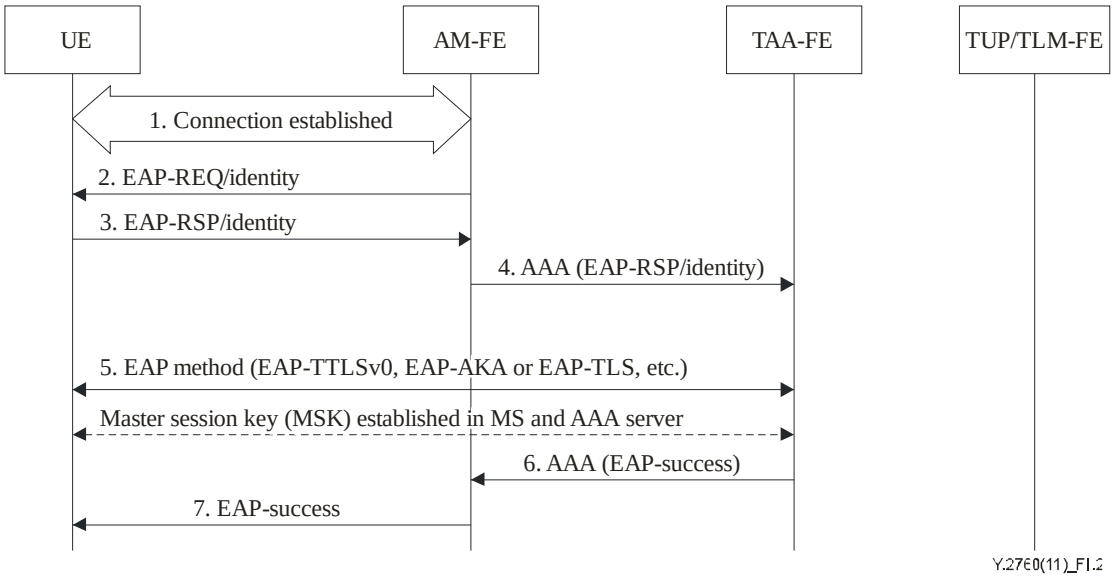

Figure I.2 – Fast re-authentication procedure

1) Connection is established between the UE and the AM-FE.
2) The AM-FE sends an EAP-REQ/Identity to the UE, carrying the re-authentication id.
3) The UE sends an EAP Response/Identity message.
4) The AM-FE forwards the EAP-RSP/Identity towards the TAA-FE.
5) The key derivation and distribution process are executed. Several methods can be considered, such as EAP-AKA, EAP-TLS, etc.
6) The TAA-FE sends the EAP Success message to the AM-FE.
7) The AM-FE informs the UE of the successful authentication with the EAP Success message. Now the key exchange process, based on EAP, has been successfully completed, and the UE and the AM-FE share the keying material derived during that exchange.

I.3 Example of host-based mobility

For MIPv4, the IP mobility security is based on MIP authentication extensions as defined in [b-IETF RFC 3344]. The IP mobility signalling messages shall be protected between the UE and the node acting as a HA (i.e., MLM-FE) using the MIP authentication extensions, and optionally between the UE and the node acting as a FA (i.e., MLM-FE).

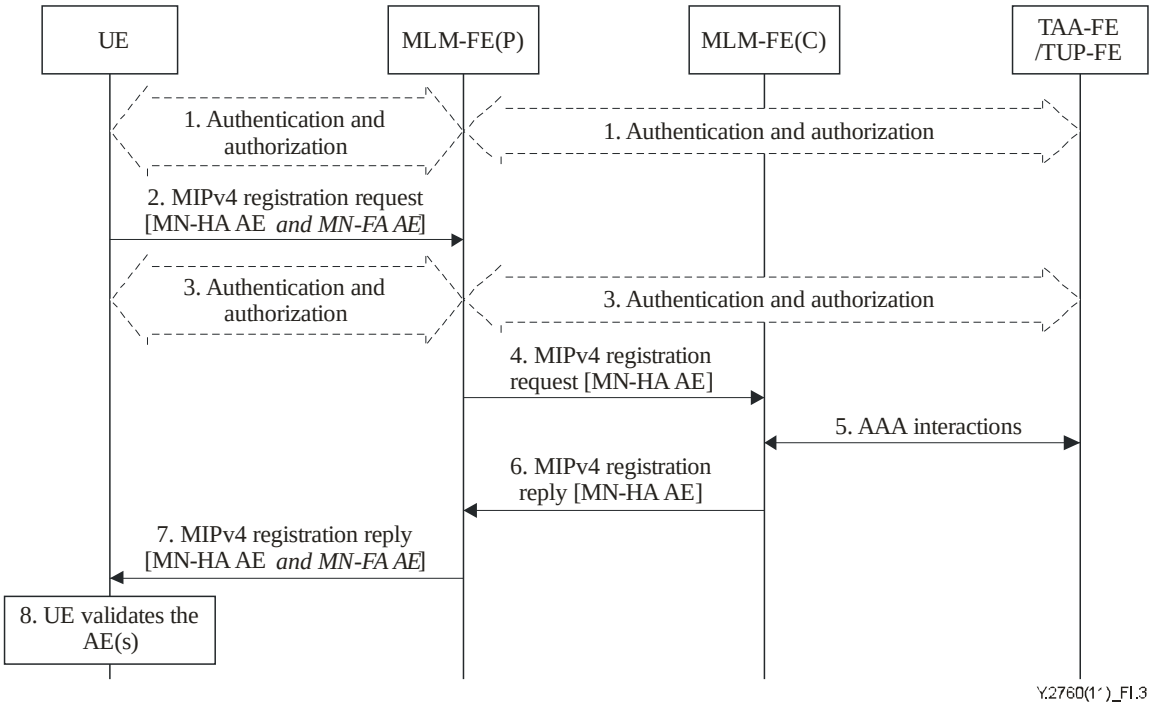

Figure I.3 – MIPv4 boostrapping procedure

The MIPv4 boostrapping procedure depicted in Figure I.3 is as follows:

1) Authentication and authorization are created between the UE and the MLM-FE with the help of the TAA-FE/TUP-FE.

2) The UE sends a Registration Request (RRQ) message to the FA (MLM-FE). The UE includes the MN-HA authentication extension (AE) and optionally the MN-FA authentication extension (AE) as specified in [b-IETF RFC 3344].

3) The RRQ triggers the access authentication procedure.

4) The FA processes the message according to [b-IETF RFC 3344] and validates the MN-FA authentication extension, if present. The FA then forwards the RRQ message to the HA (MLM-FE).

5) The selected MLM-FE obtains the authentication and authorization information from the TAA-FE/TUP-FE.

6) The MLM-FE validates the MN-HA authentication extension. After successful authentication extension validation, the MLM-FE sends a Registration Reply (RRP) to the UE through the FA.

7) The FA processes the RRP according to [b-IETF RFC 3344]. The FA then forwards the RRP message to the UE. The FA includes the MN-FA authentication extension, if the FA received the MN-FA authentication extension in the RRQ message.

8) The UE validates the MN-HA authentication extension and MN-FA authentication extension, if present.

Bibliography

[b-IETF RFC 3220] IETF RFC 3220 (2002), *IP Mobility Support for IPv4*.

[b-IETF RFC 3344] IETF RFC 3344 (2002), *IP Mobility Support for IPv4*.

[b-IETF RFC 3748] IETF RFC 3748 (2004), *Extensible Authentication Protocol (EAP)*.

[b-IETF RFC 3775] IETF RFC 3775 (2004), *Mobility Support in IPv6*.

[b-IETF RFC 4555] IETF RFC 4555 (2006), *IKEv2 Mobility and Multihoming Protocol (MOBIKE)*.

[b-IETF RFC 5213] IETF RFC 5213 (2008), *Proxy Mobile IPv6*.

[b-3GPP TS 33.102] 3GPP TS 33.102 V7.1.0 (2007), *3G Security: Security Architecture*.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	**Global information infrastructure, Internet protocol aspects and next-generation networks**
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2012